An Equivalence Theorem For Regular Differential Chains

François Boulier, François Lemaire, Adrien Poteaux, Marc Moreno Maza

An Equivalence Theorem For Regular Differential Chains

François Boulier, * François Lemaire, Adrien Poteaux

Univ. Lille, CNRS, Centrale Lille, Inria, UMR 9189 - CRIStAL - Centre de Recherche en Informatique Signal et Automatique de Lille, F-59000 Lille, France

Marc Moreno Maza

Univ. Western Ontario - ORCCA, N6A 3K7 London, Ontario, Canada

Abstract

This paper provides new equivalence theorems for regular chains and regular differential chains, which are generalizations of Ritt's characteristic sets. These theorems focus on regularity properties of elements of residue class rings defined by these chains, which are revealed by resultant computations. New corollaries to these theorems have quite simple formulations.

Key words: regular chain, characteristic set, regularity, resultant, differential algebra

1. Introduction

This paper is concerned with the study of regularity properties of the images of polynomials $f \in R$ (where R is a polynomial ring in finitely many indeterminates over a commutative field of characteristic zero) in the residue class ring $R/\mathfrak{a}$ (where $\mathfrak{a}$ is a polynomial ideal defined by some given triangular polynomial system) by means of resultant computations.

In particular, our paper provides a new equivalence theorem for a restricted class of triangular systems called *regular chains*. Some new corollaries to our new theorem have quite simple formulations, which is quite surprising since triangular sets and regular chains have been extensively studied for 25 years already.

In turn, this new theorem and its corollaries have consequences for triangular systems of differential polynomials in general and the restricted class of *regular differential chains*.

* Corresponding author

Email addresses: {francois.boulier,francois.lemaire,adrien.poteaux}@univ-lille1.fr (François Lemaire, Adrien Poteaux), moreno@csd.uwo.ca (Marc Moreno Maza).

In particular, our paper provides a new equivalence theorem for regular differential chains, together with a new corollary.

1.1. Relationship with Classical Differential Algebra

The study of regular differential chains is a rather recent topic of the elimination theory of *differential algebra*, which is an algebraic theory for systems of differential polynomials founded by Ritt (1932, 1950), developed by Kolchin (1973), which has involved an elimination theory from its very beginning. Casual readers will find in Section 1.2 an academic example which illustrates its usefulness.

A regular differential chain is a concept very close to the one of a *characteristic set* of a differential ideal. Characteristic sets were introduced in Ritt (1932) already, under the name *basic set*. The term *characteristic set* itself appears in (Ritt, 1950, Chapter I) where the nonconstructive argument that any set of differential polynomials has a characteristic set permits to prove the Ritt-Raudenbush Basis Theorem and then the fact that any radical differential ideal is a unique finite intersection of prime differential ideals. Characteristic sets are then used in (Ritt, 1950, Chapter V, Constructive Methods) as a major tool for an elimination theory.

Let us review a short set of the works which led from Ritt (1950) to the concept of regular differential chain and the ones which are strongly related to technical issues addressed by this paper. All of them essentially aim at generalizing Ritt's original ideas by fixing two important drawbacks: the use, by Ritt, of factorizations over towers of algebraic extensions of the base field of the equations; and the fact that the case of several derivations — i.e. of systems of partial differential equations — is addressed much too quickly in the last chapter of his book.

Seidenberg (1956) seems to be the first one to provide an elimination theory which is factorization free and covers the case of several derivations. However, the theory of *rankings* was not yet fully developed at this time and Seidenberg restricts himself to the case of pure elimination rankings. His methods do not compute characteristic sets: instead, they are decision procedures which gather as input a basis of a *differential ideal* $\mathfrak{A}$, a differential polynomial p and return a boolean indicating whether a power of p belongs to $\mathfrak{A}$. Their complexity is very high as pointed out by Grigoriev (1987).

Rosenfeld (1959) seems to be the first one to provide the algorithmic conditions (the so-called *coherence* property) that Ritt's characteristic sets would need to fulfill in order to apply in the case of several derivations. His Lemma is formulated using the modern concept of rankings.

Kolchin (1973) provides an impressive unified presentation of the earlier works of Ritt's school and generalizes many of them. Unfortunately, his presentation of Rosenfeld's Lemma hides the algorithmic nature of this important result.

Wu (1989) and his school popularized Ritt's theory of characteristic sets by describing many applications (though the term *characteristic set* has different meanings in the texts of Ritt and Wu). Wu does not address the case of several derivations. His work was later developed by many authors such as Wang (1996), more recently Gao et al. (2009) and many others.

Fliess (1989) pointed out the conceptual importance of differential algebra in the context of control theory. This seminal work motivated a renewal of interest for Ritt's characteristic sets in the case of a single derivation. See Ollivier (1990); Ljung and Glad (1994).

Boulier (1994) and Boulier et al. (1995) developed the first factorization free elimination method (the *RosenfeldGroebner* algorithm) for differential algebra which covers also the case of several derivations, by combining Seidenberg's idea of using Hilbert's Theorem of Zeros, Rosenfeld's Lemma and Gröbner bases for the eventual simplification of polynomial systems of equations and inequations returned by the differential procedure. The *RosenfeldGroebner* algorithm gathers as input a basis of a *differential ideal* $\mathfrak{A}$, a ranking and returns a decomposition of the radical of $\mathfrak{A}$ as an intersection of differential ideals that need not be prime but are radical, as stated by the so-called Lazard's Lemma (Boulier et al., 1995, Lemma 2). However, generalizing characteristic sets methods to nonprime ideals raises specific difficulties. In particular, it becomes much more important to understand the structure of the set of the zerodivisors in rings defined by characteristic sets — which is actually the main topic of this paper. It is this difficulty which makes the proof of (Boulier et al., 1995, Lemma 2) incomplete. Morrison (1995, 1999) was the first one to provide a complete proof, and to point out the relevance of Macaulay's unmixedness Theorem not only in this theory but also in related ones, such as most of the elimination theories relying on triangular sets.

The concept of *regular chain* was introduced independently by Kalkbrener (1993); Chou and Gao (1993); Yang and Zhang (1994), as an alternative of Gröbner bases for the study of nondifferential polynomial ideals. It would be quite long to list all the works which developed this idea. Let us just cite Aubry et al. (1999), who summarized the important properties of regular chains in (Aubry et al., 1999, Theorem 6.1), with a proof which implicitly relies on Macaulay's unmixedness Theorem. In particular, it is proved that regular chains are (up to some irrelevant degree condition) characteristic sets, in the sense of Ritt, of the polynomial ideals that they define.

Lemaire (2002) then introduced the concept of *regular differential chain*, formulated a version of *RosenfeldGroebner* that returns them and proved that they are characteristic sets, in the sense of Ritt, of the differential polynomial ideals that they define. The study of the regular chains theory in the differential framework was then developed in many articles Hubert (2000); Bouziane et al. (2001); Wang (2000); Golubitsky et al. (2007); Boulier et al. (2010); Golubitsky et al. (2009) and synthetized in many tutorials such as Sit (2002); Hubert (2003b,a).

1.2. An Academic Example

Regular differential chains are sets of differential polynomials returned by differential elimination procedures such as the `RosenfeldGroebner` function of the MAPLE `DifferentialAlgebra` package, which was developed by Boulier and Cheb-Terrab (2008) and followed an earlier package developed by Boulier and Hubert (1996). In order to motivate readers, here is a small academic example, carried out by the package.

The variable `sys` is assigned a system of polynomial PDE, in jet notation. The equations (the sign "$=0$" is omitted but the polynomials are viewed as left-hand sides of equations) are polynomials. The two *differential indeterminates* u and v represent unknown functions of the two independent variables x and y. The constant 1 represents the constant function of the two variables x and y, equal to 1. The symbol `u[x,y]` denotes the *derivative* $\partial^2 u(x,y)/(\partial x\,\partial y)$. In commutative algebra, polynomials belong to polynomial rings. In differential algebra, *differential polynomials* belong to *differential polynomial rings*. Such a differential polynomial ring is assigned to the `R` variable.

```
> with (DifferentialAlgebra):
> R := DifferentialRing(derivations = [x,y], blocks = [[v,u]]);
                              R := differential_ring
> sys := [u[x]^2-4*u, u[x,y]*v[y]-u+1, v[x,x]-u[x]];
                             2
          sys := [u[x]  - 4 u, u[x, y] v[y] - u + 1, v[x, x] - u[x]]
```

There exists a notion of *leading derivative* of a differential polynomial. This notion is by no means intrinsic. It is defined by an ordering (a *ranking*) on the set of all the derivatives of the differential indeterminates. In the variable `R` above, a ranking was defined together with the more mathematical differential polynomial ring. The following command returns the differential polynomials of `sys` in "solved form" i.e. as equations, with the leading derivatives on the left-hand sides and differential fractions on the right-hand sides.

```
> Equations(sys, R, solved);
                                                 -u + 1      2
                [v[x, x] = u[x], u[x, y] = - ------, u[x]  = 4 u]
                                               v[y]
```

The following command shows that there exists an elimination procedure (a close algorithm is detailed by Boulier (2006)) which takes as input 1) a set of differential polynomials, 2) a ranking. It returns a list of *regular differential chains* which provide much structural information on the solutions of the input system of PDE.

```
> ideal := RosenfeldGroebner(sys, R);
                      ideal := [regular_differential_chain]
```

The following commands assign the unique regular differential chain of the list to `ideal` and display the four differential polynomials which constitute it, in "solved" form.

```
> ideal := ideal[1]:
> Equations(ideal, solved);
                               -u[x] u[y] u + u[x] u[y]      2            2
[v[x, x] = u[x], v[y] = -1/4 ------------------------, u[x]  = 4 u, u[y]  = 2 u]
                                          u
```

The computed regular differential chain permits to expand solutions of the initial system into formal power series, from given initial values [1]. Initial values cannot be chosen freely. The constraints they must satisfy are provided by the regular differential chain: a property quite related to the issue of consistent initial values for numerically solving differential algebraic equations. The following command assigns to `iv` a set of admissible initial values, expressed using three arbitrary constants.

```
> iv := [u=c[0]^2, u[y]=sqrt(2)*c[0], u[x]=2*c[0], v=c[1], v[x]=c[2]];
                    2          1/2
   iv := [u = c[0] , u[y] = 2    c[0], u[x] = 2 c[0], v = c[1], v[x] = c[2]]
```

With a more classical notation, these initial values are

$$u(0,0) = c_0^2\,, \quad \frac{\partial u}{\partial y}(0,0) = \sqrt{2}\,c_0\,, \quad \frac{\partial u}{\partial x}(0,0) = 2\,c_0\,, \quad v(0,0) = c_1, \quad \frac{\partial v}{\partial x}(0,0) = c_2\,.$$

[1] This possibility holds in general, whatever the number of derivations. However, in general, the formal power series may depend on infinitely many initial values i.e. on arbitrary functions.

The following command uses them for expanding formal power series solutions of the regular differential chain stored in `ideal`, up to degree 3.

```
> sols := PowerSeriesSolution(ideal, 3, iv);
```

```
                          /                  1/2\
                          |        2  1/2   2   |                          2
sols := [v(x, y) = c[1] + |1/2 c[0]  2    - ----| y + c[2] x + 1/2 c[0] y
                          \                  2  /
                                    1/2  3      2    1/2  2       3
       1/2                    2   2    y    x y    2    x  y    x
    + 2    c[0] x y + c[0] x  + ------- + ---- + --------- + ----,
                                   12       2         2        3
                                                      2
                 2    1/2                          y      1/2        2
   u(x, y) = c[0]  + 2    c[0] y + 2 c[0] x + ---- + 2    x y + x ]
                                                      2
```

Our example is very particular because all solutions are polynomials. The next commands show that the above polynomials are solutions of our input system: the three differential polynomials of `sys` are translated into a more traditional form in `sys_diff`; then, they are evaluated at `sols`, yielding zero.

```
> sys_diff := NormalForm (sys, R, notation=diff);
```

```
             /d         \2
sys_diff := [|-- u(x, y)|  - 4 u(x, y),
             \dx        /
    /  2          \                              / 2          \
    | d           | /d         \                 |d           |   /d         \
    |----- u(x, y)| |-- v(x, y)| - u(x, y) + 1, |--- v(x, y)| - |-- u(x, y)|]
    \dy dx        / \dy        /                 |  2         |   \dx        /
                                                 \dx         /
```

```
> expand (eval (sys_diff, sols));
```

```
                                  [0, 0, 0]
```

1.3. Novelty and Structure of This Paper

Sections 2 to 8 are concerned with topics which apply as well to the nondifferential as to the differential case.

In the nondifferential context, our paper provides the following new results. Theorem 21 is new (though some of its equivalences are not). Its corollaries: Propositions 23 and 26 are new also.

Section 2 provides some algebraic preliminaries. Section 3 recalls basic properties of resultants. Triangular sets and regular chains are presented in Section 4. Section 5 provides a key theorem (Theorem 11) which, strictly speaking, is not new, but was so far only published in conference or tutorial papers. Section 6 provides a few corollaries to Theorem 11 which apply to general triangular systems. Section 7 provides a few corollaries to Theorem 11 which apply to regular chains. This section contains Theorem 21 and Propositions 23 and 26.

The literature involves so many important works on triangular sets, regular chains and resultants that it is not possible to provide a detailed comparison in this introduction. For this reason, a detailed comparison with earlier works is postponed to Section 8. We

take this opportunity to provide, in Proposition 27, the first complete proof of a popular algorithmic test which appears in Bouziane et al. (2001); Sit (2002).

Sections 9 to 10 are specifically dedicated to differential algebra.

In the differential context, our paper provides the following new results. Proposition 32 and Theorem 37 are new. Proposition 38, which is a corollary to Theorem 37 is new also.

Section 9 introduces regular differential chains and provides our new results. A comparison with earlier works is postponed to Section 10.

2. Preliminaries

An element a of a commutative ring R is a zerodivisor if there exists some nonzero $b \in R$ such that $a\,b = 0$. Thus zero is a zerodivisor (Zariski and Samuel, 1958, I, 5, page 8). An element a which is not a zerodivisor of R is said to be a *regular* element of R.

Some propositions of this paper involve statements such as "a polynomial f is zero (or a zerodivisor) in $R/\mathfrak{a}$ (R being a polynomial ring, $\mathfrak{a}$ being an ideal of R) if and only if f is reduced to zero (by some reduction process)". The word "zero" is used twice, here, but has different meanings. The expression "f is zero in $R/\mathfrak{a}$" should actually be written "the image of f by the canonical ring homomorphism $R \to R/\mathfrak{a}$ is zero" or, "f belongs to the ideal $\mathfrak{a}$". Similarly, the expression "f is a zerodivisor in $R/\mathfrak{a}$" should actually be written "the image of f by the canonical ring homomorphism $R \to R/\mathfrak{a}$ is a zerodivisor" or, "f is a zerodivisor modulo the ideal $\mathfrak{a}$". These are the properties for which we want a decision procedure: testing zero needs not be obvious in this context. The other expression "f is reduced to zero" means that the reduction process, which is a computational procedure in R, transforms f to zero, syntactically: in this context, testing zero is straightforward.

In this paper, a very important operation on ideals is the *saturation* of an ideal $\mathfrak{a}$ by some $h \in R$ (more precisely, by the multiplicative family of R generated by h). It is the ideal

$$\mathfrak{a} : h^\infty = \{f \in R \mid \exists\, d \geq 0\,,\ h^d\, f \in \mathfrak{a}\}\,.$$

We have $\mathfrak{a} \subset \mathfrak{a} : h^\infty$. This construct somehow encodes the "division by h" since $f \in \mathfrak{a} : h^\infty$ whenever $h\, f \in \mathfrak{a} : h^\infty$. If $\mathfrak{q}$ is a *primary* ideal of a ring R (Zariski and Samuel, 1958, III, 9, page 152) and $\mathfrak{p} = \sqrt{\mathfrak{q}}$ is its *associated prime ideal*, then $\mathfrak{q} : h^\infty = \mathfrak{q}$ if and only if $h \notin \mathfrak{p}$ and $\mathfrak{q} : h^\infty = R$ if $h \in \mathfrak{p}$. Therefore, in Nötherian rings, where every proper ideal $\mathfrak{a}$ has an irredundant representation $\mathfrak{a} = \cap_{i=1}^r \mathfrak{q}_i$ as an intersection of primary ideals (Zariski and Samuel, 1958, IV, 4, The Lasker-Nöther Theorem, page 208), the ideal $\mathfrak{a} : h^\infty$ is the intersection of the primary ideals $\mathfrak{q}_i$ such that $h \notin \sqrt{\mathfrak{q}_i}$ (see (Hubert, 2003a, Proposition 2.1)). The ideals $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ are called the associated prime ideals of $\mathfrak{a}$ (Zariski and Samuel, 1958, IV, 5, page 211).

Therefore, since, in Nötherian rings, the set of the zerodivisors of $R/\mathfrak{a}$ ($\mathfrak{a}$ proper) is the union of the associated prime ideals of $\mathfrak{a}$ (Zariski and Samuel, 1958, IV, 6, Corollary 3 to Theorem 11, page 214), we see that

(1) $\mathfrak{a} : h^\infty = \mathfrak{a}$ if and only if h is a regular element of $R/\mathfrak{a}$;
(2) h is a regular element of $R/(\mathfrak{a} : h^\infty) = R/\mathfrak{a} : h^\infty$, provided that h is not zero in $R/\mathfrak{a}$;
(3) if all primary components of $\mathfrak{a}$ share some common property then all primary components of $\mathfrak{a} : h^\infty$ share also this property. We will meet two examples: 1) the case of $\mathfrak{a}$ being a radical ideal (all its primary components are prime) and 2) the case of $\mathfrak{a}$ being unmixed (all its associated prime ideals have the same dimension).

3. Classical Properties of The Resultant

We provide slight generalizations of basic properties of the usual resultant of two polynomials. Our generalizations aim at covering cases which are usually not considered, such as one of the two polynomials being zero. We exclude, however, the case of two polynomials of degree less than or equal to zero i.e. two constant polynomials. Let f and g be two polynomials of $R[x]$, where R is a unitary ring of characteristic zero:

$$f = a_m\, x^m + \cdots + a_1\, x + a_0\,, \quad g = b_n\, x^n + \cdots + b_1\, x + b_0\,.$$

If f or g is zero, then the resultant of f and g is taken to be zero. Assume that f and g are nonzero and that at least one of them has positive degree. Then, the resultant of f and g is the determinant of the Sylvester matrix $S(f, g)$ of f and g, which has dimensions $(m+n)\times(m+n)$ and rows, from top down $x^{n-1}\, f, \ldots, x\, f, f, x^{m-1}\, g, \ldots, x\, g, g$. See (Basu et al., 2003, 4.2, page 105).

Lemma 1. *Assume f is nonzero and $n = 0$ (i.e. $g = b_0$). Then* $\mathrm{res}(f, g, x) = g^m$. *In particular, if $m = 1$ then* $\mathrm{res}(f, g, x) = g$.

Proof. The Lemma is clear if $g = 0$. Otherwise, expand the determinant of the Sylvester matrix, which is diagonal. □

Lemma 2. *Assume R is a domain and let K denote its fraction field. Let f and g be two polynomials of $R[x]$, not both zero. Then* $\mathrm{res}(f, g, x) = 0$ *if and only if f and g have a common factor in $K[x]$.*

Proof. The Lemma is clear if f or g is zero. Otherwise, see (Basu et al., 2003, 4.2, Proposition 4.15, page 106). □

Lemma 3. *Let R be a ring. If f and g are nonzero polynomials of $R[x]$ then there exists two polynomials $u, v \in R[x]$ with* $\deg(u) < n$ *and* $\deg(v) < m$ *such that* $\mathrm{res}(f, g, x) = u\, f + v\, g$.

Proof. See (Basu et al., 2003, 4.2, Proposition 4.18, page 108). □

The following Lemma generalizes (Basu et al., 2003, 4.2, Proposition 4.20, page 109) and deserves a proof.

Lemma 4. *Let f, g be two polynomials of $R[x]$. Let $\phi : R \to S$ be a ring homorphism such that $\phi(a_m) \neq 0$. Extend ϕ to a ring homomorphism $R[x] \to S[x]$. Then* $\phi(\mathrm{res}(f, g, x)) = \phi(a_m)^{n-t}\, \mathrm{res}(\phi(f), \phi(g), x)$.

Proof. If g is zero, then so is $\phi(g)$ and both resultants are zero. Assume g nonzero. Developing the determinant of $S(f, g)$ w.r.t. its last row, we see that any monomial of the resultant admits a coefficient of g as a factor. Thus, if $\phi(g)$ is zero, i.e. if ϕ maps all the coefficients of g to zero, then $\mathrm{res}(f, g, x) = 0$ and the Lemma holds.

Assume g and $\phi(g)$ are nonzero. If the ring homomorphism ϕ, which does not annihilate a_m, does not annihilate b_n either, then $\phi(S(f, g)) = S(\phi(f), \phi(g))$ and the Lemma is proved. Assume $\deg(\phi(g)) = t < n$. Then the Sylvester matrix $S(\phi(f), \phi(g))$ appears as the $(m + t) \times (m + t)$ submatrix of $\phi(S(f, g))$ (Fig. 1) at the bottom-right corner. Developing the determinant of $\phi(S(f, g))$ w.r.t. its $n - t$ first columns, we see that $\phi(\mathrm{res}(f, g, x)) = \phi(a_m)^{n-t}\, \mathrm{res}(\phi(f), \phi(g), x)$. □

$$\phi(S(f,g)) = \left(\begin{array}{cc|cccccccc}
\phi(a_m) & \cdots & \cdots & \cdots & \cdots & \phi(a_0) & 0 & \cdots & \cdots & 0 \\
0 & \ddots & & & & & \ddots & \ddots & & \vdots \\
\vdots & \ddots & \phi(a_m) & \cdots & \cdots & \cdots & \cdots & \phi(a_0) & 0 & 0 \\
\vdots & & \ddots & \ddots & & & & & \ddots & 0 \\
0 & \cdots & \cdots & 0 & \phi(a_m) & \cdots & \cdots & \cdots & \cdots & \phi(a_0) \\
0 & 0 & \phi(b_t) & \cdots & \cdots & \cdots & \phi(b_0) & 0 & \cdots & 0 \\
0 & & \ddots & \ddots & & & & \ddots & \ddots & \vdots \\
\vdots & & & \ddots & \ddots & & & & \ddots & 0 \\
0 & \cdots & \cdots & \cdots & 0 & \phi(b_t) & \cdots & \cdots & \cdots & \phi(b_0)
\end{array}\right) \begin{array}{l} \left.\vphantom{\begin{array}{c}a\\a\\a\\a\\a\end{array}}\right\} n-t \\ \left.\vphantom{\begin{array}{c}a\\a\\a\\a\\a\end{array}}\right\} t \\ \left.\vphantom{\begin{array}{c}a\\a\\a\\a\\a\end{array}}\right\} m \end{array}$$

Fig. 1. The image by ϕ of the Sylvester matrix $S(f,g)$.

4. Triangular Sets and Regular Chains

Let K be a commutative field of characteristic zero and $R = K[t_1, \ldots, t_m, x_1, \ldots, x_n]$ be a polynomial ring in $n+m$ indeterminates. The set $X = \{t_1, \ldots, t_m, x_1, \ldots, x_n\}$ of all indeterminates is assumed to be totally ordered in such a way that $x_1 < x_2 < \cdots < x_n$. To each polynomial $p \in R \setminus K$, one associates its *leading variable*, denoted $\mathrm{ld}\, p$, which is the highest variable $y \in X$ such that $\deg(p, y) > 0$. We are mostly concerned with a triangular set $A = \{p_1, \ldots, p_n\}$ of R such that $\mathrm{ld}\, p_k = x_k$. Unless the opposite is specified, we will always tacitly assume that triangular sets are nonempty. The *initial* of p_k, denoted i_k, is the leading coefficient of p_k w.r.t. its leading variable; the *separant* of p_k is the polynomial $s_k = \partial p_k / \partial x_k$, for each $1 \leq k \leq n$. To each triangular set A, one may associate the ideal $\mathrm{sat}\,(A) = (A) : (i_1 \cdots i_n)^\infty$. We will denote it $\mathfrak{a}$. Similarly, if A' is another triangular set, the ideal $\mathrm{sat}\,(A')$ will be denoted $\mathfrak{a}'$. This notation holds throughout the paper, except in Section 5, where gothic letters $\mathfrak{a}$ and $\mathfrak{a}'$ hold a different meaning.

The following Proposition is easy.

Proposition 5. *Let A be a triangular set, $1 \leq k \leq n$ be an index and $f \in R$ be such that $\mathrm{res}(f, p_k, x_k)$ is regular in $R/\mathfrak{a}$.*

Then f is regular in $R/\mathfrak{a}$.

Proof. If $\mathfrak{a} = R$ then $R/\mathfrak{a}$ involves no regular element and the Proposition trivially holds. Assume $\mathfrak{a}$ is proper. Denote $\mathfrak{p}$ any of its associated prime ideals. By Lemma 3 and the fact that $p_k \in \mathfrak{p}$, $\mathrm{res}(f, p_k, x_k) \notin \mathfrak{p}$, we see that $f \notin \mathfrak{p}$. Thus f is regular in $R/\mathfrak{a}$. □

Regular chains were first defined by Kalkbrener (1993); Chou and Gao (1993); Yang and Zhang (1994). See Aubry et al. (1999) for a thorough analysis of this concept.

Definition 6. A triangular set is said to be a *regular chain* if the initial i_k of p_k is regular in $R/\mathrm{sat}\,(p_1, \ldots, p_{k-1})$ for $2 \leq k \leq n$.

In particular, every singleton $A = \{p_1\}$ is a regular chain. The next Lemma is nothing but a restatement of Definition 6.

Lemma 7. *Let A be a triangular set, $R' = K[t_1, \ldots, t_m, x_1, \ldots, x_{n-1}]$ and $A' = A \cap R'$.*
Then A is a regular chain if and only if $n = 1$ or $n > 1$, the set A' is a regular chain and i_n is regular in $R'/\mathfrak{a}'$.

We now introduce the resultant of a polynomial by a triangular set.

Definition 8. Let A be a possibly empty triangular set and $f \in R$. The *resultant of f by A*, denoted $\mathrm{res}(f, A)$, is defined as follows:
(1) if $A = \varnothing$ then $\mathrm{res}(f, A) = f$;
(2) if $A = \{p_1, \ldots, p_n\}$ then $\mathrm{res}(f, A) = \mathrm{res}(\mathrm{res}(f, p_n, x_n), \{p_1, \ldots, p_{n-1}\})$.

The two following Lemmas are easy.

Lemma 9. *Let A_1 and A_2 be two possibly empty triangular sets such that any element of A_2 has leading variable strictly greater than any element of A_1.*
Then $\mathrm{res}(f, A_1 \cup A_2) = \mathrm{res}(\mathrm{res}(f, A_2), A_1)$.

Lemma 10. *Let A be a triangular set. For any $f \in R$ we have* $\mathrm{res}(f, A) \in K[t_1, \ldots, t_m]$.

5. The Unmixedness Property of Ideals Defined by Triangular Sets

An ideal of R is said to be *unmixed* if all its associated prime ideals have the same dimension (Zariski and Samuel, 1958, VII, 7, page 196).

The following Theorem already appears in (Boulier et al., 2006, Theorem 1.6). Its main ingredient is Macaulay's unmixedness Theorem, whose importance in the theory addressed in this paper was first pointed out by Morrison (1995, 1999). In the particular case of h being the product of the initials of A, it is (Hubert, 2003a, Theorem 4.4). See Section 8 for more references.

Theorem 11. *Let A be a triangular set, h denote either the product of its initials or the product of its separants and $\mathfrak{a} = (A) : h^\infty$. Assume $\mathfrak{a}$ is proper.*
Then, the ideal $\mathfrak{a}$ is unmixed. Moreover, if $\mathfrak{p}$ is an associated prime ideal of $\mathfrak{a}$ then $\dim \mathfrak{p} = m$ *and* $\mathfrak{p} \cap K[t_1, \ldots, t_m] = (0)$.

The rest of this section is entirely dedicated to the proof of Theorem 11.

Denote $\varphi : R \to h^{-1} R$ the localization at h. With the terminology of Zariski and Samuel, $h^{-1} R = R_M$ where M denotes the multiplicative family generated by h. Extended and contracted ideals (Zariski and Samuel, 1958, IV, 8) are taken with respect to φ and the ideal $\mathfrak{a} = (A) : h^\infty$ is a contracted ideal i.e. $\mathfrak{a} = \mathfrak{a}^{ec}$. The extended ideal $\mathfrak{a}^e$ is the ideal generated by $A/1 = \{p_1/1, \ldots, p_n/1\}$ in $h^{-1} R$.

Let us now introduce the ring $R' = R[x_{n+1}]$, the polynomial $p_{n+1} = h\, x_{n+1} - 1$ and the ideal $\mathfrak{a}' = (A, p_{n+1})$ of R'. Let $\pi : R' \to R'/(p_{n+1})$ denote the quotient of R' by the ideal (p_{n+1}). These two constructs are related by the ring isomorphism: $h^{-1} R \simeq R'/(p_{n+1})$. Indeed, every element of $h^{-1} R$ is a fraction f/h^d with $f \in R$ and corresponds to the equivalence class of $f\, x_{n+1}^d$ modulo (p_{n+1}).

The two ideals $\mathfrak{a}^e$ and $\pi\, \mathfrak{a}'$ are the same ideal, since they share a generating family: A.

Lemma 12. *The ideal $\mathfrak{a}'$ is proper.*

Proof. Since $\mathfrak{a} = \mathfrak{a}^{ec}$ is assumed to be proper, so is $\mathfrak{a}^e$. Since $\pi\,\mathfrak{a}' = \mathfrak{a}^e$ the ideal $\mathfrak{a}'$ is proper also. □

The next Proposition already appears in Chou and Gao (1993) or as (Kalkbrener, 1993, Theorem 3.1), in the case of $\mathfrak{a} = \mathrm{sat}\,(A)$.

Proposition 13. *We have* $\dim \mathfrak{a}' = m$. *If* $\mathfrak{p}'$ *is an isolated prime ideal of* $\mathfrak{a}'$ *then* $\dim \mathfrak{p}' = m$ *and* $\mathfrak{p}' \cap K[t_1, \ldots, t_m] = (0)$.

Proof. The ideal $\mathfrak{a}'$ is proper by Lemma 12. Applying (Zariski and Samuel, 1958, VII, 7, Theorem 22, page 196) (the principal ideal theorem) with [2] $(R, r, s, \mathfrak{A}) = (R', n+m+1, n+1, \mathfrak{a}')$, we see that every isolated prime ideal of $\mathfrak{a}'$ has dimension $\geq m$. Since the dimension of an ideal is the maximum of the dimensions of its associated prime ideals, we see that $\dim \mathfrak{a}' \geq m$.

We now claim that $\dim \mathfrak{a}' \leq m$. Let $\mathfrak{p}'$ be an associated prime ideal of $\mathfrak{a}'$ and consider some polynomial $p_i \in A$. Dropping the index i for legibility, let us write

$$p = a_d\, x^d + a_{d-1}\, x^{d-1} + \cdots + a_1\, x + a_0\,.$$

Because of the triangular nature of A, the coefficients

$$a_d, a_{d-1}, \ldots, a_0 \in K[t_1, \ldots, t_m, x_1, \ldots, x_{i-1}]\,.$$

We have $p \in \mathfrak{p}'$ and, depending on the definition of h, either

$$a_d \notin \mathfrak{p}'\,, \quad \text{or} \quad d\, a_d\, x^{d-1} + (d-1)\, a_{d-1}\, x^{d-2} + \cdots + a_1 \notin \mathfrak{p}'\,.$$

This implies that, in $R'/\mathfrak{p}'$, the polynomial p cannot become a trivial relation: in the first case, the degree of p cannot decrease while, in the second, it cannot decrease down to zero. Therefore $x = x_i$ must be algebraic over $t_1, \ldots, t_m, x_1, \ldots, x_{i-1}$ in $R'/\mathfrak{p}'$. Putting this remark in an inductive argument, we see that $x_1, \ldots, x_n$ are algebraic over $t_1, \ldots, t_m$ in $R'/\mathfrak{p}'$. Thus $\dim \mathfrak{p}' \leq m$.

Combining both inequalities, we have $\dim \mathfrak{p}' = m$ for all isolated prime ideals of $\mathfrak{a}'$ hence $\dim \mathfrak{a}' = m$. Considering again the arguments developed in the claim, we immediately see also that, if $\mathfrak{p}'$ is an isolated prime of $\mathfrak{a}'$ then $\mathfrak{p}' \cap K[t_1, \ldots, t_m] = (0)$. □

Proposition 14. *The ideal* $\mathfrak{a}'$ *is unmixed. If* $\mathfrak{p}'$ *is an associated prime ideal of* $\mathfrak{a}'$ *then* $\dim \mathfrak{p}' = m$ *and* $\mathfrak{p}' \cap K[t_1, \ldots, t_m] = (0)$.

Proof. By Proposition 13 and (Zariski and Samuel, 1958, VII, 13, Theorem 26, page 203) (Macaulay's unmixedness Theorem) with $(R, \mathfrak{A}, n, h) = (R', \mathfrak{a}', m+n+1, n+1)$. □

We are now ready to prove Theorem 11. Recall that $\mathfrak{a}'$ is supposed to be proper.

Proof. Let $\mathfrak{a}' = \cap_{i=1}^r \mathfrak{q}'_i$ be an irredundant primary representation of $\mathfrak{a}'$ and $\mathfrak{p}'_i = \sqrt{\mathfrak{q}'_i}$.

Let us apply (Zariski and Samuel, 1958, IV, 5, Remark concerning passage to a residue class ring, page 213) with $(R, \mathfrak{a}, \mathfrak{b}) = (R', \mathfrak{a}', (p_{n+1}))$. We see that $\pi\,\mathfrak{a}' = \cap_{i=1}^r (\pi\,\mathfrak{q}'_i)$ is

[2] The left-hand side symbols correspond to the book notations. The right-hand side ones correspond to our notations.

an irredundant primary representation of $\pi\,\mathfrak{a}'$ and that the $\pi\,\mathfrak{p}'_i$ are the associated prime ideals of $\pi\,\mathfrak{a}'$.

Using Proposition 14 and the fact that the π ring homomorphism removes one indeterminate and one polynomial, one sees that each prime ideal $\pi\,\mathfrak{p}'$ (dropping the index i), satisfies $\dim \pi\,\mathfrak{p}' = m$ and (with a slight abuse of notation) $\pi\,\mathfrak{p}' \cap K[t_1, \ldots, t_m] = (0)$.

Recall the ring isomorphism between $h^{-1}\,R$ and $R'/(p_{n+1})$. We have $\mathfrak{a} = \mathfrak{a}^{ec}$ and $\mathfrak{a}^e = \pi\,\mathfrak{a}'$. Let us apply (Zariski and Samuel, 1958, IV, 10, Theorem 17, page 225) with $(R, \mathfrak{a}, M) = (R, \mathfrak{a}, \{h^d \mid d \geq 0\})$. Then $\mathfrak{a} = \cap_{i=1}^{r} (\pi\,\mathfrak{q}'_i)^c$ is an irredundant primary representation of $\mathfrak{a}$. A polynomial f belongs to some $(\pi\,\mathfrak{q}')^c$ (dropping the index i) if, and only if, the fraction $f/1 \in \pi\,\mathfrak{q}'$. Thus $\dim(\pi\,\mathfrak{p}')^c = m$ and $(\pi\,\mathfrak{p}')^c \cap K[t_1, \ldots, t_m] = (0)$.

The ideal $\mathfrak{a}$ is thus unmixed. Its associated prime ideals all have dimension m and do not contain any nonzero element of $K[t_1, \ldots, t_m]$. $\square$

The following Theorem is known as Lazard's Lemma. See (Boulier et al., 1995, Lemma 2), (Boulier et al., 2009, Section 2), (Boulier et al., 2006, Theorem 2.1) and Morrison (1995, 1999). It appears also as (Hubert, 2003a, Theorem 7.5). Variants of this Theorem also appear in earlier works such as (Lazard, 1991, Proposition 5.1) and (Moreno Maza, 1997, Theorem III.5). See Section 8 for more references.

Theorem 15. *Let A be a triangular set and h be the product of the separants of A. Then the ideal $(A) : h^\infty$ is radical.*

Proof. Denote $\mathfrak{a} = (A) : h^\infty$ in R and $\mathfrak{a}_0 = (A) : h^\infty$ in $R_0 = K(t_1, \ldots, t_m)[x_1, \ldots, x_n]$. To prove that $\mathfrak{a}$ is radical, it is sufficient to prove that the total quotient ring of $R/\mathfrak{a}$, denoted $\mathrm{Fr}(R/\mathfrak{a})$, does not involve any nilpotent element. Since a direct product (or sum) of fields does not involve any nilpotent element, it is sufficient to prove that $\mathrm{Fr}(R/\mathfrak{a})$ is isomorphic to such a ring. $\mathrm{Fr}(R/\mathfrak{a})$ is equal to $(M/\mathfrak{a})^{-1}\,R/\mathfrak{a}$ where M is the multiplicative family of the elements of R which are regular in $R/\mathfrak{a}$. By Theorem 11, the nonzero elements of $K[t_1, \ldots, t_m]$ belong to M. Therefore, inverting these elements first, we conclude that $\mathrm{Fr}(R/\mathfrak{a}) \simeq \mathrm{Fr}(R_0/\mathfrak{a}_0)$.

It is thus sufficient to prove that $R_0/\mathfrak{a}_0$ is a direct sum of fields. This we do by induction on n. This ring can be constructed incrementally as S_n defined by:

$$S_0 = K(t_1, \ldots, t_m)\,, \quad S_i = S_{i-1}[x_i]/(p_i) : s_i^\infty\,,$$

where $s_i = \partial p_i / \partial x_i$ is the separant of p_i.

The basis $n = 0$ is trivial.

Assume S_{n-1} is a direct sum of fields $K_1 \oplus \cdots \oplus K_r$. Then S_n is isomorphic to the direct sum $(1 \leq j \leq r)$ of the rings $K_j[x_n]/(p_n) : s_n^\infty$.

Thus, in $K_j[x_n]$, the ideal $(p_n) : s_n^\infty$ is generated by the product of the irreducible simple factors of p_n. It is thus the intersection of the maximal ideals $\mathfrak{m}_\ell$ generated by these factors. According to the Chinese Remainder Theorem (Zariski and Samuel, 1958, III, 13, Theorem 32, page 178), $K_j[x_n]/(p_n) : s_n^\infty$ is isomorphic to the direct sum of the fields $K_j[x_n]/\mathfrak{m}_\ell$. Since direct sums are associative, the ring S_n itself is a direct sum of fields. $\square$

6. Corollaries for Ideals Defined by Triangular Sets

In this section, the gothic letters $\mathfrak{a}, \mathfrak{a}', \ldots$ recover the meaning introduced in Section 4 i.e. $\mathfrak{a} = \mathrm{sat}\,(A)$, $\mathfrak{a}' = \mathrm{sat}\,(A')$, ...

The following Proposition is part of (Chen et al., 2007, Theorem 1).

Proposition 16. *Let A be a triangular set. Assume that for each $2 \leq \ell \leq n$ we have* $\mathrm{res}(i_\ell, A)$ *regular in $R/\mathfrak{a}$.*

Then A is a regular chain.

Proof. The proof is by induction on $n = |A|$.

Basis: the case $n = 1$. The Proposition trivially holds since every singleton is a regular chain.

General case: $n > 0$. Denote $R' = K[t_1, \ldots, t_m, x_1, \ldots, x_{n-1}]$. Assume inductively that the Proposition holds for each triangular set with less than n elements. The assumption stated in the Proposition implies that $\mathrm{res}(i_\ell, A)$ is regular in $R/\mathfrak{a}$ for $2 \leq \ell < n$. These resultants, which belong to $K[t_1, \ldots, t_m]$ (Lemma 10) must then be nonzero. Since none of the initials of A depends on x_n, Lemma 1 applies and there exists some nonnegative integer α such that $\mathrm{res}(i_\ell, A) = \mathrm{res}(i_\ell, A')^\alpha$. Thus $\mathrm{res}(i_\ell, A')$ is a nonzero element of $K[t_1, \ldots, t_m]$ hence a regular element of $R'/\mathfrak{a}'$ by Theorem 11, for $2 \leq \ell < n$. Thus, by the induction hypothesis, A' is a regular chain.

We thus only need to prove that i_n is regular in $R'/\mathfrak{a}'$ (Lemma 7). The assumption stated in the Proposition implies that $\mathrm{res}(i_n, A)$ is nonzero. Since this resultant belongs to $K[t_1, \ldots, t_m]$, it is regular in $R'/\mathfrak{a}'$ by Theorem 11 applied to A'. Thus A is a regular chain. □

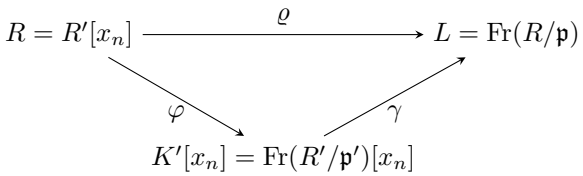
The next Proposition seems to be new.

Proposition 17. *Let A be a triangular set and $f \in R$ be regular in $R/\mathfrak{a}$.*

Then $\mathrm{res}(f, p_n, x_n)$ *is a regular element of $R/\mathfrak{a}$.*

Proof. If $\mathfrak{a} = R$ then $R/\mathfrak{a}$ does not involve any regular element and the Proposition holds. We thus assume $\mathfrak{a}$ is proper.

Let $\mathfrak{p}$ be an associated prime ideal of $\mathfrak{a}$. Denote $R' = K[t_1, \ldots, t_m, x_1, \ldots, x_{n-1}]$. Let $\mathfrak{p}' = \mathfrak{p} \cap R'$. It is a prime ideal of R'. Denote $K' = \mathrm{Fr}(R'/\mathfrak{p}')$ and $L = \mathrm{Fr}(R/\mathfrak{p})$. Let us introduce the following canonical ring homomorphisms: $\varrho : R \to L$, $\varphi : R'[x_n] \to K'[x_n]$ and $\gamma : K'[x_n] \to K'[x_n]/(\varphi\mathfrak{p})$. The following diagram commutes:



We need to prove that $\gcd(\varphi p_n, \varphi f) = 1$.

Indeed, assume this property holds. Then, φp_n and φf have no common factor hence $\mathrm{res}(\varphi f, \varphi p_n, x_n) \neq 0$ by Lemma 2. Since $\mathfrak{a}$ is saturated by the initials of A, the initial i_n of p_n has a nonzero image by φ. Lemma 4 then applies: for some nonnegative integer α we have $\varphi(\mathrm{res}(f, p_n, x_n)) = \varphi(i_n)^\alpha\ \mathrm{res}(\varphi(f), \varphi(p_n), x_n)$ thus $\varphi(\mathrm{res}(f, p_n, x_n)) \neq 0$. Since this

resultant belongs to R' and γ is the evaluation at $x_k = \varrho x_k$, we have $\gamma\varphi(\mathrm{res}(f, p_n, x_n)) = \varrho(\mathrm{res}(f, p_n, x_n)) \neq 0$. With other words, $\mathrm{res}(f, p_n, x_n)$ is a regular element of $R/\mathfrak{a}$ and the Proposition is proved.

In order to prove $\gcd(\varphi p_n, \varphi f) = 1$, we assume this is not the case and seek a contradiction. Let $g = \gcd(\varphi p_n, \varphi f)$ with $\deg g > 0$.

Denote $\bar{\mathfrak{p}}$ any associate prime ideal of $\varphi^{-1}(g)$. We have $\bar{\mathfrak{p}} \cap R' = \mathfrak{p}'$ thus $i_1, \ldots, i_n \notin \bar{\mathfrak{p}}$, $\bar{\mathfrak{p}} \cap K[t_1, \ldots, t_m] = (0)$ and $p_1, \ldots, p_{n-1} \in \bar{\mathfrak{p}}$. Since $\varphi p_n \in (g)$ we also have $p_n \in \bar{\mathfrak{p}}$ thus $\mathfrak{a} \subset \bar{\mathfrak{p}}$. Since $\dim \bar{\mathfrak{p}} = m$, we see that $\bar{\mathfrak{p}}$ is an associated prime ideal of $\mathfrak{a}$, by Theorem 11 applied to A. Now, $\varphi f \in (g)$ implies that $f \in \bar{\mathfrak{p}}$: a contradiction with the assumption that f is regular in $R/\mathfrak{a}$. Thus $\gcd(\varphi p_n, \varphi f) = 1$ and the Proposition is proved. □

Remark. It is tempting to try to generalize the last statement of the former Proposition as: "then for any $1 \leq k \leq n$ we have $\mathrm{res}(f, p_k, x_k)$ regular in $R/\mathfrak{a}$". Unfortunately, this generalization is false, even for regular chains: Consider the regular chain $A = \{p_1, p_2\} = \{(x_1 - 1)(x_1 - 3),\ x_2 - 10\,x_1\}$ and $f = x_1 + x_2 - 31$. We have f regular in $R/\mathfrak{a}$ by Condition **4** of Theorem 21 (proved later) and the fact that $\mathrm{res}(f, \{p_1, p_2\}) = -40$. However $\mathrm{res}(\mathrm{res}(f, p_1, x_1), \{p_1, p_2\}) = 0$, proving that $\mathrm{res}(f, p_1, x_1)$ is a zerodivisor in $R/\mathfrak{a}$ by Condition **4** of Theorem 21.

The next Proposition is easy. It appears as part of (Hubert, 2003a, Proposition 5.8).

Proposition 18. *Let A be a triangular set, $R' = K[t_1, \ldots, t_m, x_1, \ldots, x_{n-1}]$ and $A' = A \cap R'$.*

Then, for every associated prime ideal $\mathfrak{p}$ of $\mathfrak{a}$, the ideal $\mathfrak{p} \cap R'$ is an associated prime ideal of $\mathfrak{a}'$.

Proof. If $\mathfrak{a} = R$ then $\mathfrak{a}$ has no associated prime ideal and the Proposition holds. Thus assume that $\mathfrak{a}$ is proper.

By Theorem 11 applied to A, we have $\mathfrak{p} \cap K[t_1, \ldots, t_m] = (0)$ and $\dim \mathfrak{p} = m$. Thus the prime ideal $\mathfrak{p}'$ satisfies $\mathfrak{p}' \cap K[t_1, \ldots, t_m] = (0)$ and $\dim \mathfrak{p}' = m$ (in R'). We have $\mathfrak{a}' \subset \mathfrak{a} \cap R' \subset \mathfrak{p}'$. By Theorem 11 applied to A', the prime ideal $\mathfrak{p}'$ has the same dimension as the associated prime ideals of $\mathfrak{a}'$. It is thus one of them. □

7. Special Corollaries for Ideals Defined by Regular Chains

The following Proposition appears as (Hubert, 2003a, Proposition 5.8). A variant of it appears in (Wang, 2000, Theorem 5.1). An informal way to restate it would be: every m-dimensional zero of A' can be prolonged to an m-dimensional zero of A.

Proposition 19. *Let A be a regular chain, $R' = K[t_1, \ldots, t_m, x_1, \ldots, x_{n-1}]$ and $A' = A \cap R'$.*

Then the ideals $\mathfrak{a}$ of R and $\mathfrak{a}'$ of R' are proper.

Moreover, for every associated prime ideal $\mathfrak{p}'$ of $\mathfrak{a}'$, there exists an associated prime ideal $\mathfrak{p}$ of $\mathfrak{a}$ such that $\mathfrak{p}' = \mathfrak{p} \cap R'$.

Proof. The proof is by induction on n.

Basis: the case $n = 1$. Then $\mathfrak{a}' = (0)$ is proper. It has a single associated prime ideal $\mathfrak{p}' = (0)$. The ideal $\mathfrak{a} = \mathrm{sat}\,(p_1)$ is proper too. Its associated prime ideals, which

are generated by the irreducible factors of p_1 with positive degree in x_1, are such that $\mathfrak{p}' = \mathfrak{p} \cap R'$.

General case: $n > 1$. By induction hypothesis, $\mathfrak{a}'$ is proper. Let $\mathfrak{p}'$ be any associated prime ideal of $\mathfrak{a}'$. Since A is a regular chain, the initial i_n of p_n does not belong to $\mathfrak{p}'$. First consequence: $(\mathfrak{p}', p_n) : i_n^\infty$ is a proper ideal of R and $\mathfrak{a}$, which is included in $(\mathfrak{p}', p_n) : i_n^\infty$ is proper too. Second consequence: for each associated prime ideal $\mathfrak{p}$ of $(\mathfrak{p}', p_n) : i_n^\infty$, we have $\mathfrak{p} \cap R' = \mathfrak{p}'$ thus, by Theorem 11 applied over $\mathfrak{a}'$, $\dim \mathfrak{p} = m$ and $\mathfrak{p} \cap K[t_1, \ldots, t_m] = (0)$. By Theorem 11 again, these prime ideals $\mathfrak{p}$, which contain $\mathfrak{a}$, must be associated prime ideals of $\mathfrak{a}$. □

Remark. The previous Proposition is false for general triangular sets. Consider the triangular set $A = \{x_1^2 - 1, (x_1 - 1)(x_2 - 3)\}$. The prime ideal $\mathfrak{p}' = (x_1 - 1)$ is an associated prime ideal of $\mathfrak{a}' = (x_1^2 - 1)$. However, the ideal $\mathfrak{a} = (x_1 + 1, x_2 - 3)$, which is equal to its unique associated prime ideal $\mathfrak{p}$, does not satisfy $\mathfrak{p}' = \mathfrak{p} \cap K[x_1]$. In this example, the initial $x_1 - 1$ belongs to the associated prime ideal $\mathfrak{p}'$ of $\mathfrak{a}'$.

The next Proposition was proved in (Chen et al., 2007, Lemma 4) in the zero-dimensional case and generalized in (Boulier et al., 2011, Theorem 1). A variant of it is (Wang, 2000, Proposition 5.3).

Proposition 20. *Let A be a regular chain, $1 \leq k \leq n$ be an index and $f \in R$ be regular in $R/\mathfrak{a}$.*

Then $\operatorname{res}(f, \{p_k, \ldots, p_n\})$ *is regular in $R/\mathfrak{a}$.*

Proof. Since A is a regular chain, $\mathfrak{a}$ is necessarily proper by Proposition 19. The proof is by induction on n. The index $1 \leq k \leq n$ is fixed.

Basis: assume $n = k$. Then $\operatorname{res}(f, \{p_k, \ldots, p_n\}) = \operatorname{res}(f, p_n, x_n)$ and the proof follows from Proposition 17.

General case: assume $n > k$. Denote $R' = K[t_1, \ldots, t_m, x_1, \ldots, x_{n-1}]$ and $A' = A \cap R'$. The induction hypothesis is: if g is regular in $R'/\mathfrak{a}'$ then $\operatorname{res}(g, \{p_k, \ldots, p_{n-1}\})$ is regular in $R'/\mathfrak{a}'$.

Decompose $\operatorname{res}(f, \{p_k, \ldots, p_n\}) = \operatorname{res}(g, \{p_k, \ldots, p_{n-1}\})$ with $g = \operatorname{res}(f, p_n, x_n)$. By Proposition 17, g is regular in $R/\mathfrak{a}$. We have $g \in R'$. Since A is a regular chain, Proposition 19 applies and g is regular in $R'/\mathfrak{a}'$. By the induction hypothesis, $\operatorname{res}(f, \{p_k, \ldots, p_n\})$ is regular in $R'/\mathfrak{a}'$. This resultant belongs to R' and does not belong to any associated prime ideal $\mathfrak{p}'$ of $\mathfrak{a}'$. By Proposition 18, it does not belong to any associated prime ideal of $\mathfrak{a}$. Thus it is regular in $R/\mathfrak{a}$. □

7.1. An Equivalence Theorem for Regular Chains

Theorem 21. *Let A be a triangular set. The following conditions are equivalent:*

1 *A is a regular chain;*

2 *for each $2 \leq \ell \leq n$ and each $1 \leq k \leq n$ we have* $\operatorname{res}(i_\ell, \{p_k, \ldots, p_n\})$ *regular in $R/\mathfrak{a}$;*

3 *for each $2 \leq \ell \leq n$ we have* $\operatorname{res}(i_\ell, A) \neq 0$*;*

4 *for each $f \in R$, f is regular in $R/\mathfrak{a}$ if and only if* $\operatorname{res}(f, A) \neq 0$.

5 *for each $f \in R$,*

$$f \text{ is regular in } R/\mathfrak{a}$$
$$\Updownarrow$$
$$\text{for each } 1 \leq k \leq n,\ \operatorname{res}(f, \{p_k, \ldots, p_n\}) \text{ is regular in } R/\mathfrak{a};$$

Proof. The implication **1** ⇒ **5**. Since A is a triangular set, Proposition 5 holds and so does the bottom-up implication of Condition **5**. Assume Condition **1**. Then Proposition 20 holds and so does the top-down implication of Condition **5**.

The implication **5** ⇒ **4**. Assume Condition **5** holds. The implication ⇒ of Condition **4** trivially holds. Let us now address the implication ⇐ of Condition **4**. Assume $\mathrm{res}(f, A) \neq 0$. Then this resultant is regular in $R/\mathfrak{a}$ by Lemma 10 and Theorem 11. Thus $\mathrm{res}(f, \{p_k, \ldots, p_n\})$ is regular in $R/\mathfrak{a}$ for each $1 \leq k \leq n$ by Lemma 9 and Proposition 5. Thus f is regular in $R/\mathfrak{a}$ by Condition **5**.

The implication **4** ⇒ **3**. The ideal $\mathfrak{a}$ is saturated by the initials of A. Thus these initials are regular in $R/\mathfrak{a}$. Thus if Condition **4** holds then Condition **3** holds too.

The implication **5** ⇒ **2**. The ideal $\mathfrak{a}$ is saturated by the initials of A. Thus these initials are regular in $R/\mathfrak{a}$. Thus if Condition **5** holds then Condition **2** holds too.

The implication **2** ⇒ **3** trivially holds.

The implication **3** ⇒ **1** holds by Proposition 16. □

7.2. Every Subset of a Regular Chain is a Regular Chain

The next Lemma is new. It is a key element of the proof of Proposition 23.

Lemma 22. *Consider the following decomposition of a regular chain A, where A_1 or A_2 may be empty but $A' = A_1 \cup A_2$ may not.*

$$\underbrace{p_1, p_2, \ldots, p_k}_{A_1}, p_{k+1}, \ldots, p_{\ell-1}, \underbrace{p_\ell, \ldots, p_n}_{A_2} .$$

Let $f \in R$ be regular in $R/\mathfrak{a}$.

Then f is regular in $R/\mathfrak{a}'$. In particular, A' is a regular chain.

Proof. The set A' is triangular.

Since A is a regular chain, we have $r_2 = \mathrm{res}(f, A_2)$ regular in $R/\mathfrak{a}$ by Condition **5** of Theorem 21. By Proposition 19, we thus have r_2 regular in $R/\mathfrak{a}_1$. Since A_1 is a regular chain, we have $\mathrm{res}(r_2, A_1) \neq 0$ by the implication **1** ⇒ **4** of Theorem 21. By Lemma 9, we have $\mathrm{res}(r_2, A_1) = \mathrm{res}(f, A') \neq 0$.

The ideal $\mathfrak{a}$ is saturated by the initials of A'. Thus these initials are regular in $R/\mathfrak{a}$. The above argument thus applies to them: given any initial f of A' we have $\mathrm{res}(f, A') \neq 0$. Thus A' is a regular chain by the implication **3** ⇒ **1** of Theorem 21.

Consider again some f regular in $R/\mathfrak{a}$. In the first paragraph of the proof, we have established that $\mathrm{res}(f, A') \neq 0$. Since A' is a regular chain, f is regular in $R/\mathfrak{a}'$ by the implication **1** ⇒ **4** of Theorem 21. □

The following Proposition is new.

Proposition 23. *Let A be a regular chain and $A' \subset A$ be nonempty.*

Then A' is a regular chain. Moreover, every $f \in R$ which is regular in $R/\mathfrak{a}$ is regular in $R/\mathfrak{a}'$.

Proof. The set A' can be obtained from A by a sequence of transformations similar to the one considered in Lemma 22. The proof thus follows from successive applications of Lemma 22. □

The concept of squarefree triangular set goes back, at least, to (Lazard, 1991, Definition 3.2).

Definition 24. A regular chain A is said to be *squarefree* if, for each $1 \leq k \leq n$, the separant s_k of p_k is regular in $R/\mathfrak{a}$.

The following Proposition appears as (Hubert, 2003a, Proposition 7.6). Many variants appeared before. See Lazard (1991); Moreno Maza (1997).

Proposition 25. *If A is a squarefree regular chain then $\mathfrak{a}$ is radical.*

Proof. Since A is squarefree we have $\mathfrak{a} = \mathfrak{a} : h^\infty$ where h denotes the product of the separants of A. Thus $\mathfrak{a}$ is equal to the saturation of $\mathfrak{b} = (A) : h^\infty$ by the product of the initials of A. By Theorem 15, the ideal $\mathfrak{b}$ is radical. It is thus the intersection of its associated prime ideals. Thus $\mathfrak{a}$ is the intersection of the associated prime ideals of $\mathfrak{b}$ which do not contain any initial of A. Since every intersection of prime ideals is radical, the Proposition is proved. □

The following Proposition is new.

Proposition 26. *Let A be a regular chain and $A' \subset A$ be nonempty and such that, for every $p_k \in A'$, the separant s_k of p_k is regular in $R/\mathfrak{a}$.*

Then A' is a squarefree regular chain. In particular, every nonempty subset of a squarefree regular chain is a squarefree regular chain.

Proof. It is an immediate consequence of Proposition 23 and the definition of squarefree regular chains. □

8. Comparison with Earlier Works

Before addressing the consequences of the former sections for differential algebra, let us enter detailed comparisons between the results we have established so far and earlier works.

The study of the regularity or the invertibility of polynomials w.r.t. triangular systems and the properties of the iterated resultant of a polynomial w.r.t. triangular systems have a long history.

Recall that $\mathfrak{a} = \mathrm{sat}\,(A)$ i.e. the ideal (A) generated by the triangular set A, saturated by the multiplicative family generated by the initials of A. This ideal is implicitly supposed to be proper in the following discussion.

8.1. Earlier Works Addressing the Dimension of the Solution Set

An important set of papers focus on the properties of the solution set of triangular systems. See Lazard (1991); Kalkbrener (1993). Among them, many of studies are conducted by means of the iterated resultant. See Yang and Zhang (1994); Yang et al. (1995); Wang (2000); Yang et al. (2001). In particular, it is proved in (Kalkbrener, 1993, Theorem 3.1) and independently by Chou and Gao (1993) that the algebraic variety of $\mathfrak{a}$ is unmixed, has dimension m and that $\{t_1, \ldots, t_m\}$ provides a parametric set for its components.

In ideal theoretic terms, these results immediately imply, using (Zariski and Samuel, 1958, VII, 3, Corollary 3 to Nullstellensatz, page 167), that Property (1) below holds for any isolated associated prime ideal $\mathfrak{p}$ of $\mathfrak{a}$.

$$\dim \mathfrak{p} = m\,, \qquad \mathfrak{p} \cap K[t_1, \ldots, t_m] = (0)\,. \tag{1}$$

Our Theorem 11 actually completes these important results since 1) it establishes that Property (1) holds not only for isolated associated prime ideals of $\mathfrak{a}$ but for all associated prime ideals, which is a necessary condition, by (Zariski and Samuel, 1958, IV, 6, Corollary 3 to Theorem 11, page 214), to conclude that nonzero elements of $K[t_1, \ldots, t_m]$ are regular elements in $R/\mathfrak{a}$ — which is an issue addressed in this paper; 2) it establishes that the very same property holds not only for $\mathrm{sat}\,(A)$ but also for $(A) : h^\infty$ where h stands for the product of the separants of A.

8.2. Earlier Works Addressing the Regularity Property

Testing the regularity of polynomials w.r.t. triangular systems has been addressed in another set of papers. Comparing this paper with earlier ones requires longer developments since:

(1) some papers implicitly assume that ideals defined by triangular sets have no imbedded associated prime ideals;
(2) some papers provide alternative definitions, and meanings, to qualifiers such as "invertible" or "regular";
(3) some papers focus on ideals saturated by the separants (rather than the initials) of A.

8.2.1. Earlier Works Assuming the Nonexistence of Imbedded Primes

Papers which implicitly assume that ideals defined by triangular sets have no imbedded associated prime ideals often deduce the properties of the ring $R/\mathfrak{a}$ from the ones of $R_0/(\mathfrak{a}\, R_0)$ where $R_0 = K(t_1, \ldots, t_m)[x_1, \ldots, x_n]$. Notice now that

(1) Theorem 11 (Proposition 13 is actually sufficient) and basic results of the dimension theory (Zariski and Samuel, 1958, VII, 7, page 193) imply that if $\mathfrak{p}$ is an imbedded associated prime ideal of $\mathfrak{a}$ then $\mathfrak{p} \cap K[t_1, \ldots, t_m] \neq (0)$;
(2) using the notations of (Zariski and Samuel, 1958, IV, 9, Quotient rings, page 221) R_0 is equal to R_M, where M is the multiplicative family of the nonzero elements of $K[t_1, \ldots, t_m]$ so that the associated prime ideals of $\mathfrak{a}\, R_0$ are the associated prime ideals of $\mathfrak{a}$ which do not meet M (Zariski and Samuel, 1958, IV, 10, Theorem 17, page 225).

From the two remarks above, it immediately follows that no information on possible imbedded prime ideals of $\mathfrak{a}$ can be inferred from the study of $\mathfrak{a}\, R_0$. Thus any result which, having established that some property holds for all associated prime ideals of $\mathfrak{a}\, R_0$, concludes that the same property holds for all associated prime ideals of $\mathfrak{a}$, implicitly assumes the nonexistence of possible imbedded associated prime ideals for $\mathfrak{a}$.

8.2.2. Earlier Works Redefining Invertibility and Regularity

The following definition is (Sit, 2002, Definition 3.15, page 14). It can also be found in (Bouziane et al., 2001, page 632):

A polynomial f is said to be regular if $(\mathfrak{a}, f) \cap K[t_1, \ldots, t_m] \neq (0)$.

The article (Bouziane et al., 2001, page 632) refers to Lazard (1991) for a proof. However, we could not find any reference to this statement in Lazard's article.

Then one may wonder if it is true that a polynomial f is regular (in the above sense) if and only it is a regular element of $R/\mathfrak{a}$. Proposition 27 below proves that the answer is yes, since $\mathfrak{a}$ has no imbedded associated prime ideals. The above question is actually not addressed in Sit (2002); Bouziane et al. (2001). If we consider that it should be implicitly understood that the two notions of regularity are equivalent, then Proposition 28 below shows that these papers implicitly assume that $\mathfrak{a}$ has no imbedded associated prime ideal. An example of such an implicit assumption seems to appear in the first sentence of the proof of (Sit, 2002, Corollary 3.17, page 15).

Proposition 27. *Let A be a triangular set and $f \in R$.*

Then f is a regular element of $R/\mathfrak{a}$ if and only if $(\mathfrak{a}, f) \cap K[t_1, \ldots, t_m] \neq (0)$.

Proof. Assume f is a zerodivisor in $R/\mathfrak{a}$. Then, by (Zariski and Samuel, 1958, Corollary 3 to Theorem 11, page 214), f belongs to some associated (isolated or imbedded) prime ideal $\mathfrak{p}$ of $\mathfrak{a}$. By Theorem 11, which implies that $\mathfrak{a}$ has no imbedded prime ideal, we have $\mathfrak{p} \cap K[t_1, \ldots, t_m] = (0)$. Since $(\mathfrak{a}, f) \subset (\mathfrak{p}, f) = \mathfrak{p}$, we have $(\mathfrak{a}, f) \cap K[t_1, \ldots, t_m] \subset \mathfrak{p} \cap K[t_1, \ldots, t_m] = (0)$.

Assume now that f is a regular element of $R/\mathfrak{a}$. Then f belongs to none of the associated prime ideals of $\mathfrak{a}$. These ideals have dimension at most m by Theorem 11 (Proposition 13 is actually sufficient). Then by (Kolchin, 1973, 0, 16, Proposition 11, page 43), the radical of $(\mathfrak{a}, f)$ is an intersection of prime ideals $\mathfrak{p}_i$ $(1 \leq i \leq r)$ which have dimension at most $m - 1$. Thus there exists nonzero polynomials $g_i \in \mathfrak{p}_i \cap K[t_1, \ldots, t_m]$ for $1 \leq i \leq r$. Take $g = g_1\, g_2 \cdots g_r$. There exists an exponent α such that g^α, which is a nonzero element of $K[t_1, \ldots, t_m]$, belongs to $(\mathfrak{a}, f)$. Thus $(\mathfrak{a}, f) \cap K[t_1, \ldots, t_m] \neq (0)$. □

Proposition 28. *Let $\mathfrak{b}$ be an ideal of R. Assume* $\dim \mathfrak{p} = m$ *and* $\mathfrak{p} \cap K[t_1, \ldots, t_m] = (0)$ *for every isolated prime ideal $\mathfrak{p}$ of $\mathfrak{b}$. Assume moreover that for every $f \in R$ which is a zerodivisor in $R/\mathfrak{b}$ we have* $(\mathfrak{b}, f) \cap K[t_1, \ldots, t_m] = (0)$.

Then $\mathfrak{b}$ has no imbedded associated prime ideal.

Proof. We assume $\mathfrak{b}$ has an imbedded associated prime ideal $\mathfrak{p}$ and seek a contradiction. Then we have $\dim \mathfrak{p} < m$ hence $\mathfrak{p} \cap K[t_1, \ldots, t_m] \neq (0)$. Consider any nonzero polynomial $f \in \mathfrak{p} \cap K[t_1, \ldots, t_m]$. By (Zariski and Samuel, 1958, Corollary 3 to Theorem 11, page 214), f is a zerodivisor in $R/\mathfrak{b}$. On the one hand, $(\mathfrak{b}, f) \cap K[t_1, \ldots, t_m] = (0)$ by assumption. On the other hand, $(\mathfrak{b}, f)$ contains f hence $(\mathfrak{b}, f) \cap K[t_1, \ldots, t_m] \neq (0)$. This contradiction proves the Proposition. □

8.2.3. Earlier Works on Ideals Saturated by the Separants

It is the case of (Boulier et al., 1995, Lemma 2) i.e. Lazard's Lemma, which is our Theorem 15. The implicit assumption of the nonexistence of imbedded associated prime ideals was pointed out for the first time by Morrison (1995), then published in Morrison (1999). Many proofs were then published. See Schicho and Li (1995); Ollivier (1998)

(Boulier et al., 2009, Theorem 2.1), (Boulier et al., 2006, Theorem 2.1) and (Hubert, 2003a, Theorem 7.5). All these proofs focus on the radicality property of the ideal defined by the triangular set. A careful study of these proofs in order to find out if one of them does not need the nonexistence of imbedded primes still needs to be carried out.

8.3. Originality of our Results

Our Theorem 11 establishes the nonexistence of imbedded associated prime ideals for ideals saturated by the initials of A or by the separants of A, in a single proof. However, the result in itself is not new. It was already published as (Boulier et al., 2006, Theorem 1.6). The first proof, applying to the case of the initials only seems to be (Hubert, 2003a, Theorem 4.4). In the case of the separants, the first proof seems to be due to Morrison (1995, 1999).

The statements of our Theorem 21 seem very close to statements of earlier papers. A variant of this equivalence theorem is (Wang, 2000, Theorem 5.1). However, as we have developed above: 1) some earlier proofs suffered from the implicit assumption covered by Theorem 11 and deserve a more accurate presentation; 2) some statements which look similar at first sight are actually different (e.g. an ideal may have an unmixed algebraic variety without being unmixed).

Some of its implications are already known. The equivalence $\mathbf{1} \Leftrightarrow \mathbf{3}$ appears in (Chen et al., 2007, Theorem 1). An earlier version of this equivalence, stated in terms of *proper ascending chains* appears in (Yang and Zhang, 1994, Corollary 4, page 150). The implication $\mathbf{1} \Rightarrow \mathbf{4}$ is proved in (Chen et al., 2007, Lemma 4) in dimension zero and generalized in (Boulier et al., 2011, Theorem 1). The implication $\mathbf{4} \Rightarrow \mathbf{1}$ is proved in (Boulier et al., 2011, Lemma 5). The other equivalences $\mathbf{1} \Leftrightarrow \mathbf{2}$ and $\mathbf{1} \Leftrightarrow \mathbf{5}$ seem to be new.

Propositions 23, 26 are new. Though Proposition 27 is not new, we provide its first complete proof and analysis. All these results have interesting consequences in the differential context, as we shall see in the next section.

9. Regular Differential Chains

Reference books are the ones of Ritt (1950) and Kolchin (1973).

Let $R = K\{U\}$ be a differential polynomial ring where K is a differential field of characteristic zero, U is a finite set of differential indeterminates u_k, endowed with a finite set of derivations. Let Θ denote the multiplicative monoid of derivation operators, generated by the derivations and $\Theta^* \subset \Theta$ the set of proper derivation operators. Assume the infinite set of derivatives ΘU is ordered w.r.t. a ranking (Kolchin, 1973, I, 8, page 75) so that, given any differential polynomial $f \in R \setminus K$, its leading derivative $\mathrm{ld}\, f$ (called *leader* by Kolchin), its initial and its separant $\partial f / \partial \,\mathrm{ld}\, f$ are well defined.

In the sequel, we will often have to consider sets of differential polynomials as particular cases of sets of plain polynomials, in order to apply the results of the former sections. By a *triangular set* of differential polynomials $\{p_1, \ldots, p_n\}$ we mean a set of differential polynomials of $R \setminus K$ having pairwise distinct leading derivatives. In order to apply the results of the former sections and fit to their notations, we assume moreover that $\mathrm{ld}\, p_1 < \mathrm{ld}\, p_2 < \cdots < \mathrm{ld}\, p_n$. These leading derivatives then correspond to the variables $x_1, x_2, \ldots, x_n$. In particular, the numbering of the x is imposed by the ranking. The other derivatives occuring in the differential polynomials correspond to $t_1, \ldots, t_m$.

Consider again the example given in Section 1.2. The differential indeterminates are u and v. The monoid Θ of derivation operators is generated by two derivations δ_x, δ_y, interpreted as partial derivations with respect to two independent variables. More precisely, $\Theta = \{\delta_x^\alpha \, \delta_y^\beta \mid \alpha, \beta \in \mathbb{N}\}$. System `sys` is made of three differential polynomials with leading derivatives $u_x < u_{xy} < v_{xx}$. The ordering is imposed by the ranking defined in `R`. Two other derivatives u, v_y occur in the differential polynomials. In order to apply the results of the former sections, one should rename $x_1, x_2, x_3 = u_x, u_{xy}, v_{xx}$ and either $t_1, t_2 = u, v_y$, or $t_1, t_2 = v_y, u$ since the ordering between the t variables is irrelevant. Observe also that the set of the t variables may be enlarged with derivatives which do not occur at all in the differential polynomials.

This being understood, there is no ambiguity in a statement such as "the triangular set A of differential polynomials is a regular chain". It suffices to apply the above renaming and Definition 6. Similarly, if f is any differential polynomial, the differential polynomial $\mathrm{res}(f, A)$ is well defined, by means of Definition 8.

A differential polynomial f is said to be *partially reduced* w.r.t. a differential polynomial $p \notin K$ if f does not depend on any proper derivative of the leading derivative of p (Kolchin, 1973, I, 9, page 77).

We are mostly concerned by a triangular set A of differential polynomials of R.

Then $R_1 \subset R$ denotes the ring of the differential polynomials partially reduced w.r.t. A.

In the sequel, uppercase gothic letters denote differential ideals while lowercase ones denote nondifferential ones. In particular, we denote $\mathfrak{A}$ the differential ideal $[A] : h^\infty$ of R where h denotes the product of the initials and separants of A. We denote $\mathfrak{a} = \mathrm{sat}\,(A)$ the nondifferential ideal of R defined by A, viewed as a plain triangular set. We will sometimes consider other triangular sets A', A''. Then $\mathfrak{a}' = \mathrm{sat}\,(A')$ and $\mathfrak{a}'' = \mathrm{sat}\,(A'')$.

Let A be a triangular set of pairwise partially reduced differential polynomials. In the partial case, it may happen that there exists pairs $\{p_1, p_2\} \in A$ whose leading derivatives $\theta_1 u, \theta_2 u$ are the derivatives of some common differential indeterminate $u \in U$. Consider any such *critical pair* $\{p_1, p_2\} \subset A$. Let $\theta_{12} = \mathrm{lcm}(\theta_1, \theta_2)$. Define the Δ*-polynomial* generated by the critical pair as

$$\Delta(p_1, p_2) = s_2 \, \frac{\theta_{12}}{\theta_1} \, p_1 - s_1 \, \frac{\theta_{12}}{\theta_2} \, p_2 \, .$$

By construction, we have either $\Delta(p_1, p_2) \in K$ or $\mathrm{ld}\,\Delta(p_1, p_2) < \theta_{12} u$. Moreover, we obviously have $\Delta(p_1, p_2) \in \mathfrak{a}'$ where $A' = \{p \in \Theta A \mid \mathrm{ld}\, p \leq \theta_{12} u\}$. Thus notice the strict inequality in the next definition.

Definition 29. The critical pair $\{p_1, p_2\} \subset A$ is said to be *solved* if $\Delta(p_1, p_2) \in \mathfrak{a}'$ where $A' = \{p \in \Theta A \mid \mathrm{ld}\, p < \theta_{12} u\}$.

In the sequel, triangular sets are tacitly supposed to be nonempty.

Definition 30. A triangular set of pairwise partially reduced differential polynomials is said to be *coherent* if all its critical pairs are solved.

Definition 31. A triangular set A of pairwise partially reduced differential polynomials is said to be a *regular differential chain* if it is a coherent squarefree regular chain.

The statements of most of the following Lemmas and Propositions may somewhat look complicated because we often stress the existence of polynomial rings (usually denoted R') in finitely many derivatives. This permits us to reduce problems to Nœtherian rings hence to allow a sound use of classical commutative algebra theorems.

Lemma 32. *Let A be a triangular set of pairwise partially reduced differential polynomials and $f \in R$.*

Then there exists a finite triangular subset $A' \subset \Theta A$ and a finitely generated polynomial ring R' such that $f \in R'$, $A' \subset R'$ and $\operatorname{res}(f, A') \in R_1 \cap R'$.

Moreover, there exists a power product h of separants of A and a differential polynomial $q \in (A') \subset \mathfrak{a}'$ such that the following relation holds:

$$h\, f = \operatorname{res}(f, A') + q\,. \tag{2}$$

Proof. Given any $g \in R$ define

$$V(g) = \{w \in \Theta U \mid \deg(g, w) > 0,\ \exists\, \theta \in \Theta^*,\ p \in A,\ \text{s.t.}\ \operatorname{ld} \theta p = w\}\,.$$

We clearly have $g \notin R_1$ if and only if $V(g) \neq \varnothing$.

Consider the sequence of polynomials (r_k) defined as follows and which terminates whenever $r_k \in R_1$:

$$r_0 = f\,, \quad r_{k+1} = \operatorname{res}(r_k, \theta\, p, v)$$

where $v = \max V(r_k)$ and θp is a proper derivative of any $p \in A$ such that $\operatorname{ld} \theta p = v$. The above process eventually terminates because the sequence of the v is strictly decreasing and rankings are well orderings (Kolchin, 1973, I, 8, page 75). Property (2) follows from Lemma 3.

The set A' can be defined as the set of all the θp involved in the above process. A possible ring R' is the polynomial ring in the finitely many derivatives occuring in A' and f. □

Remark The differential polynomial $\operatorname{res}(f, A')$ mentioned in Lemma 32 is (possibly up to the sign) the *partial remainder* of f by A as defined in (Kolchin, 1973, I, 9, page 77).

9.1. Results Which do not Require Coherence

The following Proposition is new.

Proposition 33. *Let A be a squarefree regular chain of pairwise partially reduced differential polynomials and A' be any finite triangular subset of $\Theta\, A$.*

Then A' is a squarefree regular chain and $\mathfrak{a}'$ is radical.

Proof. First observe that we do not assume that $A \subset A'$. Since the elements of A are pairwise partially reduced, the set $A \cup A'$ is triangular.

Let f be any initial or separant of A'. Then f is either an initial or a separant of A and $\operatorname{res}(f, A) \neq 0$ by the implications $\mathbf{1} \Rightarrow \mathbf{3}, \mathbf{4}$ of Theorem 21 and the fact that A is a squarefree regular chain. Since the elements of A are pairwise partially reduced, f is partially reduced w.r.t. A and, by Lemma 1, there exists an exponent α such that $\operatorname{res}(f, A \cup A') = \operatorname{res}(f, A)^\alpha$. Thus $\operatorname{res}(f, A \cup A') \neq 0$. Thus $A \cup A'$ is a regular chain by

the implication **3** $\Rightarrow$ **1** of Theorem 21. Moreover, by Definition 24 and the implication **1** $\Rightarrow$ **4** of Theorem 21, the regular chain $A \cup A'$ is squarefree.

Thus A' is a squarefree regular chain by Proposition 26 and $\mathfrak{a}'$ is radical by Proposition 25. □

The following Proposition is new.

Proposition 34. *Let A be a triangular set of pairwise partially reduced differential polynomials. Assume that, for any $f \in R$ we have*

$$f \text{ is regular in } R/\mathfrak{A}$$
$$\Updownarrow$$
for any triangular finite subset $A' \subset \Theta A$ such that $\operatorname{res}(f, A') \in R_1$, $\operatorname{res}(f, A') \neq 0$.

Then A is a regular differential chain.

Proof. There exists f and A' such that $\operatorname{res}(f, A') \in R_1$ and $\operatorname{res}(f, A') \neq 0$ (take $f \in K$). Thus, using the assumption stated in the Proposition, there exists regular elements in $R/\mathfrak{A}$. Thus $\mathfrak{A}$ is proper.

The differential ideal $\mathfrak{A}$ is saturated by the initials and separants of A. Thus these initials and separants are regular in $R/\mathfrak{A}$. Since the elements of A are pairwise partially reduced, so are their initials and separants. Thus, using the assumption stated in the Proposition, for any initial or separant g of A, $\operatorname{res}(g, A) \neq 0$. Thus A is a regular chain by the implication **3** $\Rightarrow$ **1** of Theorem 21. Moreover, by Definition 24 and the implication **1** $\Rightarrow$ **4** of Theorem 21, the regular chain A is squarefree.

By Proposition 33, any finite triangular set $A' \subset \Theta A$ is a squarefree regular chain of its embedding ring R' and $\mathfrak{a}'$ is radical.

By the implication **1** $\Rightarrow$ **4** of Theorem 21, applied to A', given any $f \in R'$, we have f regular in $R'/\mathfrak{a}'$ if and only if $\operatorname{res}(f, A') \neq 0$. Thus, using the assumption stated in the Proposition, given any $f \in R'$, we have f regular in $R/\mathfrak{A}$ if and only if f is regular in $R'/\mathfrak{a}'$. Extending the polynomial ring R' if needed, $f \in R'$ is regular in $R/\mathfrak{A}$ if and only f is regular in $R'/(\mathfrak{A} \cap R')$. Therefore, the ideals $\mathfrak{A} \cap R'$ and $\mathfrak{a}'$ have the same set of associated prime ideals whence have the same radical.

Since $\mathfrak{a}'$ is radical we have $\sqrt{\mathfrak{A} \cap R'} = \mathfrak{a}'$. This property actually holds for any ring R' such that $A' \subset R'$.

Let us now consider the particular case of $f = \Delta(p_1, p_2)$ where $\{p_1, p_2\} \subset A$ is a critical pair. Denote $\operatorname{ld} p_1 = \theta_1 u$, $\operatorname{ld} p_2 = \theta_2 u$ and $\theta_{12} = \operatorname{lcm}(\theta_1, \theta_2)$. If $f = 0$ then the critical pair is solved. If $f \neq 0$ then $\operatorname{ld} f < \theta_{12} u$ and A' can be chosen so that its elements only depend on derivatives less than or equal to $\operatorname{ld} f$ (Lemma 32). Since $f \in \mathfrak{A} \cap R'$, by the result established above, we have $f \in \mathfrak{a}'$ and the critical pair is solved.

Thus all critical pairs of A are solved, A is a coherent squarefree regular chain and the Proposition is proved. □

9.2. Results which Require Coherence

The following Proposition is an easy Corollary to Rosenfeld's Lemma (Rosenfeld, 1959, Lemma).

Proposition 35. *Let A be a regular differential chain.*

Then $\mathfrak{A} \cap R_1 = \mathfrak{a}$.

Proof. Since A is a coherent set of pairwise partially reduced differential polynomials, Rosenfeld's Lemma (Rosenfeld, 1959, Lemma) applies and we have $\mathfrak{A} \cap R_1 = (A) : h^\infty$ where h denotes the product of the initials and separants of A. Since A is a squarefree regular chain $(A) : h^\infty = \mathfrak{a}$. □

The following Lemma is an easy generalization of Proposition 35.

Lemma 36. *Let A be a regular differential chain and $f \in R$. Let A' and R' as in Lemma 32. Assume moreover that $A \subset A'$.*
Then $\mathfrak{A} \cap R' = \mathfrak{a}'$.

Proof. The inclusion $\mathfrak{a}' \subset \mathfrak{A} \cap R'$ is clear.

To prove the converse inclusion, let us consider some $g_0 \in \mathfrak{A} \cap R'$. By Lemma 32, there exists a power product h of separants of A, a differential polynomial $g_1 \in R' \cap R_1$ (take $g_1 = \mathrm{res}(g_0, A' \setminus A)$) and a differential polynomial $r \in \mathfrak{a}'$ such that

$$h\, g_0 = g_1 + r\,. \tag{3}$$

Since $g_0 \in \mathfrak{A}$ we have $g_1 \in \mathfrak{A}$. By Proposition 35, $g_1 \in \mathfrak{a}$. Thus $g_1 \in \mathfrak{a} \cap R'$. Since $A \subset A'$, we have $g_1 \in \mathfrak{a}'$. Using (3), we conclude that $g_0 \in \mathfrak{a}'$ and the Lemma is proved. □

9.3. An Equivalence Theorem for Regular Differential Chain

Theorem 37. *Let A be a triangular set of differential polynomials pairwise partially reduced. The following conditions are equivalent:*
1 *A is a regular differential chain;*
2 *A is coherent and, for each $1 \leq \ell \leq n$ and each $1 \leq k \leq n$ we have $\mathrm{res}(i_\ell, \{p_k, \ldots, p_n\})$ and $\mathrm{res}(s_\ell, \{p_k, \ldots, p_n\})$ regular in $R/\mathfrak{a}$;*
3 *A is coherent and, for each $1 \leq \ell \leq n$ we have $\mathrm{res}(i_\ell, A) \neq 0$ and $\mathrm{res}(s_\ell, A) \neq 0$;*
4 *for each $f \in R$,*

$$f \text{ is regular in } R/\mathfrak{A}$$
$$\Updownarrow$$
for any triangular finite subset $A' \subset \Theta A$ such that $\mathrm{res}(f, A') \in R_1$, $\mathrm{res}(f, A') \neq 0$.

Proof. The implication **1** ⇒ **2**. Assume Condition **1** holds. A is coherent. The initials of A are regular in $R/\mathfrak{a}$ since $\mathfrak{a}$ is saturated by them. Since A is a squarefree regular chain, its separants are regular in $R/\mathfrak{a}$ too by Definition 24. Thus by the implication **1** ⇒ **5** of Theorem 21 we see that Condition **2** of Theorem 37 holds.

The implication **2** ⇒ **3** is clear.

The implication **3** ⇒ **1**. Assume Condition **3** holds. Then A is a regular chain by the implication **3** ⇒ **1** of Theorem 21. By Definition 24 and the implication **1** ⇒ **4** of Theorem 21, the regular chain A is squarefree. Since A is coherent, we see that Condition **1** of Theorem 37 holds.

The implication **4** ⇒ **1** is Proposition 34.

The implication **1** ⇒ **4**. Assume Condition **1** holds. Then every set A' considered in Condition **4** is a squarefree regular chain by Proposition 33. By the implication **1** ⇒ **4** of Theorem 21 applied to any such A', we see that f is regular in $R'/\mathfrak{a}'$ if and only if $\mathrm{res}(f, A') \neq 0$, where R' is any finitely generated polynomial ring containing f, A' and $\mathrm{res}(f, A')$. Extending R' if needed, f is regular in $R/\mathfrak{A}$ if and only if f is regular in

$R'/(\mathfrak{A} \cap R')$. Assuming moreover $A \subset A'$ and using Lemma 36, we see that f is regular in $R/\mathfrak{A}$ if and only if $\mathrm{res}(f, A') \neq 0$. We have thus proved Condition **4** of Theorem 37 holds provided that $A \subset A'$. This implies that the implication from bottom-up of Condition **4** holds in general. The top-down implication of Condition **4** follows from the fact that, if A' is a regular chain, $\mathrm{res}(f, A') \neq 0$ and $A'' \subset A'$ then $\mathrm{res}(f, A'') \neq 0$ by Proposition 23. Condition **4** of Theorem 37 thus holds. □

The following Proposition is new.

Proposition 38. *Let A be a regular differential chain and A' be a coherent nonempty subset of A.*

Then A' is a regular differential chain. Moreover, every $f \in R$ which is regular in $R/\mathfrak{A}$ is regular in $R'/\mathfrak{A}'$.

Proof. By Proposition 26, the set A' is a squarefree regular chain. Since it is coherent, A' is regular differential chain. The last statement follows from the implication $\mathbf{1} \Rightarrow \mathbf{4}$ of Theorem 37 applied to A and A' and the fact that $\Theta A' \subset \Theta A$. □

10. Comparison with Earlier Works

There are much less works in the differential case than in the nondifferential one. In particular, the regularity property of differential polynomials w.r.t. triangular systems of differential polynomials was almost not studied.

The use of iterated resultants for studying systems of polynomial differential equations is however not new. Examples can be found in the works of Bächler et al. (2012); Robertz (2014).

The definition of regular differential chains was introduced by Li and Wang (1999) and, independently, by Lemaire (2002).

In our Theorem 37, almost all equivalences are new. The implication $\mathbf{1} \Rightarrow \mathbf{4}$ appears in (Boulier et al., 2011, Theorem 3). Particularly interesting is the implication $\mathbf{4} \Rightarrow \mathbf{1}$, which applies to a differential system which is not assumed to be coherent.

The key Proposition 33, which is a consequence of our algebraic results as well as Proposition 38 are new.

References

Aubry, P., Lazard, D., Moreno Maza, M., 1999. On the Theories of Triangular Sets. Journal of Symbolic Computation 28, 105–124.

Bächler, T., Gerdt, V., Lange-Hegermann, M., Robertz, D., 2012. Algorithmic Thomas Decomposition of Algebraic and Differential Systems. Journal of Symbolic Computation 47 (10), 1233–1266.

Basu, S., Pollack, R., Roy, M.-F., 2003. Algorithms in Real Algebraic Geometry. Vol. 10 of Algorithms and Computation in Mathematics. Springer Verlag.

Boulier, F., 1994. Étude et implantation de quelques algorithmes en algèbre différentielle. Ph.D. thesis, Université Lille I, 59655, Villeneuve d'Ascq, France, `http://tel.archives-ouvertes.fr/tel-00137866`.

Boulier, F., May 2006. Réécriture algébrique dans les systèmes d'équations différentielles polynomiales en vue d'applications dans les Sciences du Vivant. Mémoire d'habilitation à diriger des recherches. Université Lille I, LIFL, 59655 Villeneuve d'Ascq, France. http://tel.archives-ouvertes.fr/tel-00137153.

Boulier, F., Cheb-Terrab, E., 2008. DifferentialAlgebra. Package of MapleSoft MAPLE standard library since MAPLE 14.

Boulier, F., Hubert, É., 1996. diffalg. Package of MapleSoft MAPLE standard library from MAPLE V to MAPLE 13.

Boulier, F., Lazard, D., Ollivier, F., Petitot, M., 1995. Representation for the radical of a finitely generated differential ideal. In: ISSAC'95: Proceedings of the 1995 international symposium on Symbolic and algebraic computation. ACM Press, New York, NY, USA, pp. 158–166, http://hal.archives-ouvertes.fr/hal-00138020.

Boulier, F., Lazard, D., Ollivier, F., Petitot, M., 2009. Computing representations for radicals of finitely generated differential ideals. Applicable Algebra in Engineering, Communication and Computing 20 (1), 73–121, (1997 Techrep. IT306 of the LIFL). URL http://dx.doi.org/10.1007/s00200-009-0091-7

Boulier, F., Lemaire, F., Moreno Maza, M., 2006. Well known theorems on triangular systems and the D^5 principle. In: Proceedings of Transgressive Computing 2006. Granada, Spain, pp. 79–91, http://hal.archives-ouvertes.fr/hal-00137158.

Boulier, F., Lemaire, F., Moreno Maza, M., 2010. Computing differential characteristic sets by change of ordering. Journal of Symbolic Computation 45 (1), 124–149, doi:10.1016/j.jsc.2009.09.04.

Boulier, F., Lemaire, F., Sedoglavic, A., 2011. On the Regularity Property of Differential Polynomials Modulo Regular Differential Chains. In: Proceedings of Computer Algebra in Scientific Computing, LNCS 6885. Kassel, Germany, pp. 61–72, http://hal.archives-ouvertes.fr/hal-00599440.

Bouziane, D., Kandri Rody, A., Maârouf, H., 2001. Unmixed–Dimensional Decomposition of a Finitely Generated Perfect Differential Ideal. Journal of Symbolic Computation 31, 631–649.

Chen, C., Lemaire, F., Moreno Maza, M., Pan, W., 2007. Comprehensive Triangular Decompositions. In: Proceedings of CASC'07. pp. 73–101.

Chou, S.-C., Gao, X.-S., 1993. On the dimension of an arbitrary ascending chain. Chinese Bulletin of Science 38, 799–904.

Fliess, M., 1989. Automatique et corps différentiels. Forum Math. 1, 227–238.

Gao, X.-S., Van Der Hoeven, J., Yuan, C. M., Zhang, G. L., 2009. Ritt-Wu's Characteristic Set Method for Differential-Difference Polynomial Systems. Journal of Symbolic Computation 44 (9), 1137–1163.

Golubitsky, O., Kondratieva, M., Moreno Maza, M., Ovchinnikov, A., 2007. Bounds and algebraic algorithms in differential algebra: the ordinary case. In: Decker, W., Dewar, M., Kaltofen, E., Watt, S. M. (Eds.), Challenges in Symbolic Computation Software. No. 06271 in Dagstuhl Seminar Proceedings. Internationales Begegnungs und Forschungszentrum für Informatik (IBFI), Schloss Dagstuhl, Germany.

Golubitsky, O., Kondratieva, M., Ovchinnikov, A., 2009. Algebraic transformation of differential characteristic decompositions from one ranking to another. J. Symb. Comput. 44 (4), 333–357.

Grigoriev, D. Y., 1987. Complexity of quantifier elimination in the theory of ordinary differential equations. Vol. 378 of Lecture Notes in Computer Science. Springer Verlag, pp. 11–25.

Hubert, É., 2000. Factorization free decomposition algorithms in differential algebra. Journal of Symbolic Computation 29 (4,5), 641–662.

Hubert, É., 2003a. Notes on triangular sets and triangulation–decomposition algorithm I: Polynomial Systems. In: Proceedings of Symbolic and Numerical Scientific Computing. No. 2630 in LNCS. pp. 1–39.

Hubert, É., 2003b. Notes on triangular sets and triangulation–decomposition algorithm II: Differential Systems. Symbolic and Numerical Scientific Computing 2001, 40–87.

Kalkbrener, M., 1993. A Generalized Euclidean Algorithm for Computing Triangular Representations of Algebraic Varieties. Journal of Symbolic Computation 15, 143–167.

Kolchin, E. R., 1973. Differential Algebra and Algebraic Groups. Academic Press, New York.

Lazard, D., 1991. A new method for solving algebraic systems of positive dimension. Discrete Applied Mathematics 33, 147–160.

Lemaire, F., January 2002. Contribution à l'algorithmique en algèbre différentielle. Ph.D. thesis, Université Lille I, 59655, Villeneuve d'Ascq, France, (in French).

Li, Z., Wang, D., 1999. Coherent, regular and simple systems in zero decompositions of partial differential systems. Systems Science and Mathematical Sciences 12, 43–60.

Ljung, L., Glad, S. T., 1994. On global identifiability for arbitrary model parametrisations. Automatica 30, 265–276.

Moreno Maza, M., 1997. Calculs de Pgcd au–dessus des Tours d'Extensions Simples et Résolution des Systèmes d'Équations Algébriques. Ph.D. thesis, Université Paris VI, France.

Morrison, S., december 1995. Yet another proof of Lazard's lemma. private communication.

Morrison, S., 1999. The Differential Ideal $[P] : M^\infty$. Journal of Symbolic Computation 28, 631–656.

Ollivier, F., 1990. Le problème de l'identifiabilité structurelle globale : approche théorique, méthodes effectives et bornes de complexité. Ph.D. thesis, École Polytechnique, Palaiseau, France.

Ollivier, F., october 1998. A proof of Lazard's lemma. private communication.

Ritt, J. F., 1932. Differential equations from the algebraic standpoint. Vol. 14 of American Mathematical Society Colloquium Publications. American Mathematical Society, New York.

Ritt, J. F., 1950. Differential Algebra. Vol. 33 of American Mathematical Society Colloquium Publications. American Mathematical Society, New York.

Robertz, D., 2014. Formal Algorithmic Elimination for PDEs. Vol. 2121 of Lecture Notes in Mathematics. Springer Verlag.

Rosenfeld, A., 1959. Specializations in differential algebra. Trans. Amer. Math. Soc. 90, 394–407.

Schicho, J., Li, Z., august 1995. A construction of radical ideals in polynomial algebra. Tech. rep., RISC, Johannes Kepler University, Linz, Austria.

Seidenberg, A., 1956. An elimination theory for differential algebra. Univ. California Publ. Math. (New Series) 3, 31–65.

Sit, W., 2002. The Ritt–Kolchin theory for differential polynomials. In: L. Guo and P. J. Cassidy and W. F. Keigher and W. Y. Sit (Ed.), Proceedings of the international workshop: Differential Algebra and Related Topics. pp. 1–70.

Wang, D., 1996. An elimination method for differential polynomial systems I. Systems Science and Mathematical Sciences 9 (3), 216–228.

Wang, D., 2000. Computing Triangular Systems and Regular Systems. Journal of Symbolic Computation 30, 221–236.

Wu, W., 1989. On the foundation of algebraic differential geometry. Mechanization of Mathematics, research preprints 3, 2–27.

Yang, L., Hou, X., Xia, B., 2001. A complete algorithm for automated discovering of a class of inequality-type theorems. Science in China Series F: Information Sciences 44 (1), 33–49.

Yang, L., Zhang, J., 1994. Searching dependency between algebraic equations: an algorithm applied to automated reasoning. Artificial Intelligence in Mathematics, 147–1561991 version available at `streaming.ictp.trieste.it/preprints/P/91/006.pdf`.

Yang, L., Zhang, J., Hou, X., 1995. An Efficient Decomposition Algorithm for Geometry Theorem Proving Without Factorization. Proceedings of ASCM, 33–41.

Zariski, O., Samuel, P., 1958. Commutative Algebra. Van Nostrand, New York, Also volumes 28 and 29 of the Graduate Texts in Mathematics, Springer Verlag.